

Checklist

5.27 – Leren van informatiebeveiligingsincidenten

Thema: Organisatorisch | ISO 27002: 5.27 | Gerelateerd: 5.26, 5.28

Doelstelling

Aantonen dat de organisatie lessen trekt uit informatiebeveiligingsincidenten om beveiligingsmaatregelen te verbeteren en herhaling te voorkomen.

Post-incident review

- ☐ Vindt na elk significant incident een post-incident review (PIR) plaats?
- ☐ Is de PIR-procedure beschreven en worden uitkomsten gedocumenteerd?
- ☐ Worden oorzaken (root causes) van incidenten systematisch geanalyseerd?
- ☐ Worden zowel technische als organisatorische oorzaken onderzocht?
- ☐ Is vastgelegd binnen welke termijn een PIR wordt uitgevoerd na het incident?

Verbeteracties

- ☐ Worden uit elke PIR concrete verbeteracties afgeleid?
- ☐ Worden verbeteracties toegewezen aan een verantwoordelijke met een deadline?
- ☐ Worden verbeteracties gemonitord op uitvoering en afdoening?
- ☐ Worden systeemconfiguraties, procedures en beleid bijgewerkt op basis van lessen?

Kennisdeling

- ☐ Worden lessen uit incidenten gedeeld met relevante medewerkers en teams?
- ☐ Worden geanonimiseerde incidentcasussen gebruikt in bewustwordingstraining?
- ☐ Worden lessen gedeeld met ketenpartners of sectorale netwerken waar relevant?
- ☐ Is er een kennisbank of incidentendatabase voor opgebouwde ervaring?

Rapportage en trends

- ☐ Worden incidenttrends periodiek geanalyseerd en gerapporteerd aan management?
- ☐ Is er aandacht voor structurele kwetsbaarheden die uit meerdere incidenten blijken?
- ☐ Worden incidentlessen meegenomen in de jaarlijkse risicoanalyse?



Wordt de effectiviteit van verbeteracties geëvalueerd na implementatie?

Verantwoordelijke:	_____	Datum controle:	_____
Afdeling:	_____	Score:	___ / 21
Reviewcyclus:	☐ Jaarlijks ☐ Na wijziging ☐ Na incident		Status: ☐ Voldoet ☐ Actiepunt ☐ N.v.t.